Certificate Management Entities for Connected Vehicle Program

Task 2: Organizational Models for Certificate Management

December 9, 2011
Public Webinar

Table of Contents

Introduction to Connected Vehicle Program and Certificate Management Entity Options

Communications Framework within Connected Vehicle Environment

- The Connected Vehicle Program is focused on implementing a secure communications system that will support Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications and become a network that is trusted by the public
- A secure communications network for certificate management will facilitate message exchange in a trusted environment. Safety, environmental, and mobility messages are among the key messages that need to be communicated

Requirements for Certificate Management

This current project is focused on developing options for organizational and operational models to administer and manage the Certificate Management Entities (CMEs) that will:

- Ensure secure exchange of data between vehicles, and between vehicles and roadside equipment as part of the Connected Vehicle Program
- Define roles and responsibilities of the CMEs
- Develop rules of operation, SOPs, and decision-making standards for the CMEs
- Recommend rules of access to the certificate management system
- Identify resource requirements and cost estimates
- Develop implementation plans for creating and operating CMEs

Project Approach

Perform Critical Research

- Reviewed documentation
- Documented the perspectives of multiple stakeholder groups:
  - RITA ITS JPO
  - VIIC/CAMP
  - AASHTO
  - Trucking Industry reps & FMCSA
  - NHTSA
  - Transit Industry reps & FTA
- Researched comparative industry practices and organizations
  - Federal PKI Policy Authority
  - International Registration Plan
  - E-ZPass toll system
  - Smart Grid

Develop Organizational Models

- Developed assumptions regarding policies
- Analyzed sub-functions and activities of required functions
- Identified 15 total possible model options
- Collapsed range of possible models
- Built in requisite elements to models:
  - Communications security
  - Privacy protection
  - Governance models
  - Cost estimates (relative)
  - Roles and responsibilities

Evaluate, Refine, and Select

- Continue to build detailed roles, responsibilities, policy needs, and governance guidance for select models
- Incorporate feedback from stakeholders and USDOT staff
- Select final model to be developed for subsequent testing

A select group of models will be chosen to be developed in more detail by March 2012

Stakeholder Perspectives

Stakeholder outreach provided insight on multiple stakeholder perspectives and desires for the Certificate Management Entities

Stakeholder Group	Areas of Interest
VIIC/CAMP	▸ Multiple separate entities with different governance structures ▸ Backwards compatibility of system technology ▸ Accounting for and managing jurisdictional boundaries/barriers
AASHTO	▸ Functional responsibilities ▸ Sources of funding ▸ CMEs integrated into and built on existing standards
RITA	▸ Levels of privacy and security of system ▸ Sustainable financing/cost implications of system

Stakeholder Group	Areas of Interest
Trucking Industry reps and FMCSA	▸ Type and amount of PII collected ▸ Potential differences in trucking involvement versus light vehicle ▸ Sources of funding
NHTSA	▸ Integrating security credentials with existing organization (e.g., vehicle registration/VIN) ▸ Privacy principles (anonymity and adherence to other frameworks)
Transit Industry reps and FTA	▸ Certificate revocation ▸ Accounting for and managing jurisdictional boundaries/barriers ▸ Sources of funding

Technical Considerations ("Knowns")

Public Key Infrastructure (PKI)

- PKI is the governing paradigm for the communications security within the entire system and the communications and exchange of certificates
- Linkage Authority (LA) was introduced due to the scale of the system and the large amount of certificates being signed, distributed, monitored, etc.

Personally Identifiable Information (PII)

- The amount of personally identifiable information collected will be what is necessary for system functionality and effective operations.

System Nomenclature

- The "activation infrastructure" is the system that activates the OBE. It includes a Certification Authority for Activation (CA_{ACT}) and Registration Authority for Activation (RA_{ACT}) that are separate from the CA and RA of the pseudo system
- The "pseudo" system is operated on an ongoing basis to verify, exchange, distribute, monitor and accept certificates between vehicles and also between vehicles and Road Side Equipment (RSE)

Working Assumptions (for “Unknowns”)

While several technical and policy decisions that will guide the CMEs are still being explored, the consultant followed certain working assumptions based on current research and perspectives

Organizational Boundaries

- The best way to ensure privacy and protect security of communications is with distinct organizational boundaries. For some functions that is the only acceptable method of control

Fair Information Practices Principles (FIPPs)

- FIPPs (NIST SP 800-53 Draft, Appendix J) will provide the framework for analysis of privacy protection
- FIPPs are comprehensive and subsume the VII Privacy Principles Framework

Certificate Signing Request (CSR) / Seed Key

- For all new vehicles, the CSR/Seed Key will be activated at the dealer upon the vehicle arriving at the lot
- For after-market devices, CSR/Seed Key will happen upon installation of the device
- There will be a CRL specific to CSR certificates

Certificate Revocation List (CRL)

- The linked identifier from the LA allows for efficient revocation of all certificates in a batch
- There are two entries in the CRL – one for regular certificates and one for back-up certificates
- OBE holds a dynamic list of revoked certificates

Opt In vs. Mandated

- Initially, participation in the system could be potentially mandated for new cars, and after-market devices will likely represent an opt in choice

Linkage Authority (LA)

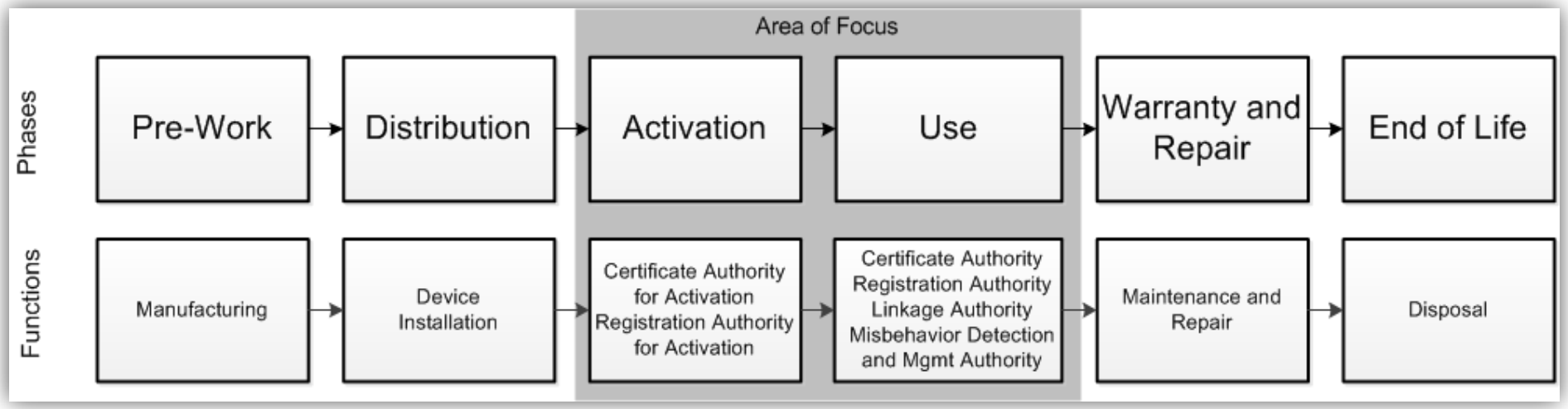
- There are two LAs in order to ensure that no one function (LA) can track a vehicle based on the data they have
- An individual certID is derived from two LA certIDs

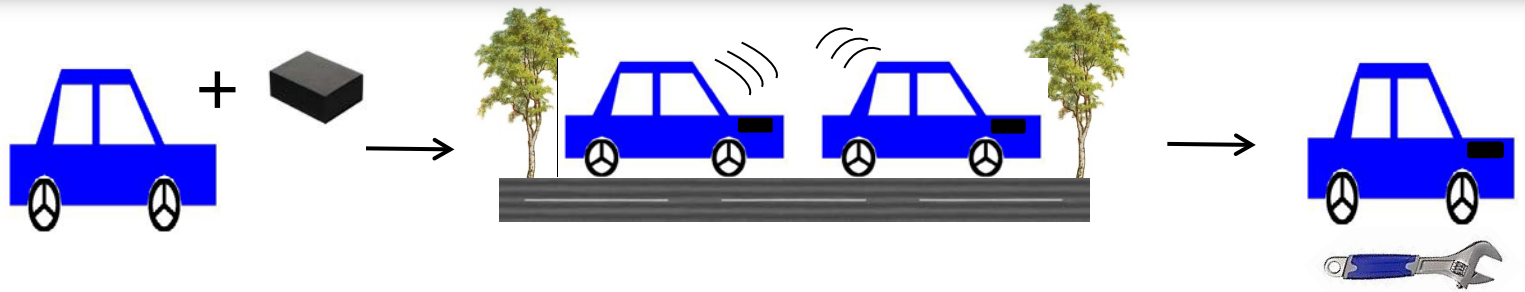
Life Spans of Certificates

- Short term certificates = 5 minutes
- Overlap of short term certificates = 30 seconds
- Long term/back up certificates = 1 year
- Batches of five-minute certificates are downloaded once a year = 105,000 certificates
- Decryption keys are provided once a month to unlock monthly groups of the full yearly batch
- CSR life span = greater than1 year but less than 2 years

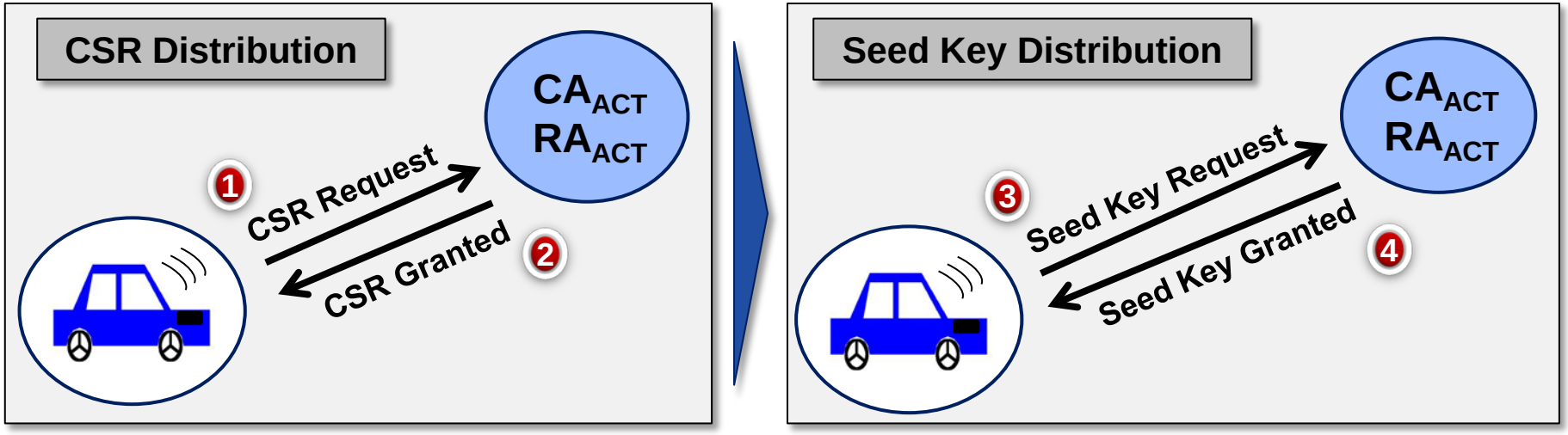
Life Cycle of On Board Equipment

- In developing models for how certificates will be assigned, distributed, and monitored throughout the connected vehicle system, it is important to remember that there exist other stages of an entire life cycle of the On Board Equipment (OBE)
- This project is primarily concerned with the functions and activities associated with the Use Phase and Activation Phase of the life cycle





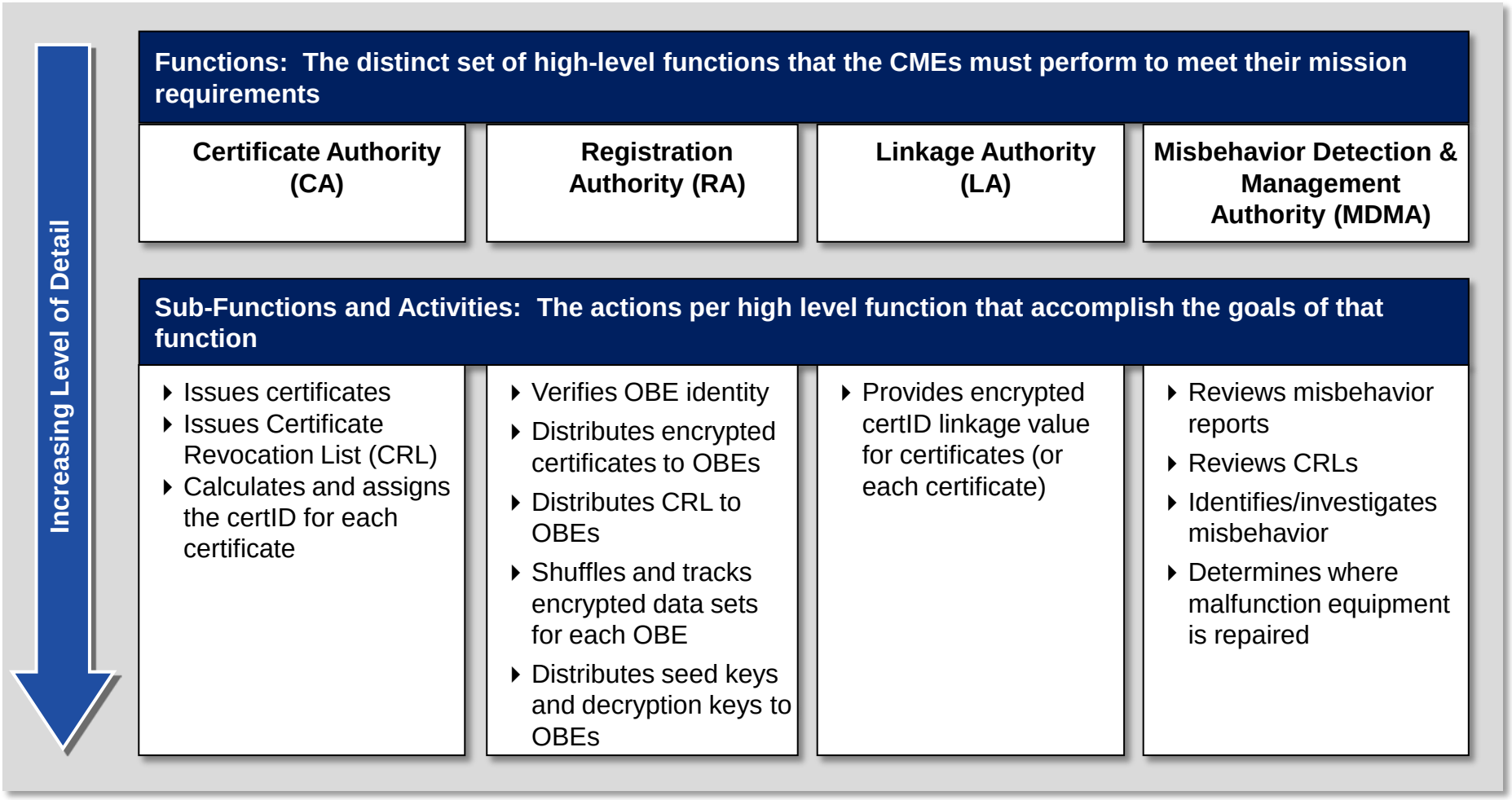
Functions and Process of Activation



- The CSR certificate contains the OBE identity. This is the place in the system where any PII will be collected and stored
- There is no need for RA_{ACT} and CA_{ACT} to be separated as in the pseudo system because the CSR is not intended to provide any anonymity (as do the 105K certificates issued in the pseudo system) – the CSR is not used in location-based communications

This process implies a separate entity (or inclusion in an existing organization) for the CA_{ACT} and RA_{ACT} functions, apart from the various entities needed to manage the pseudo system

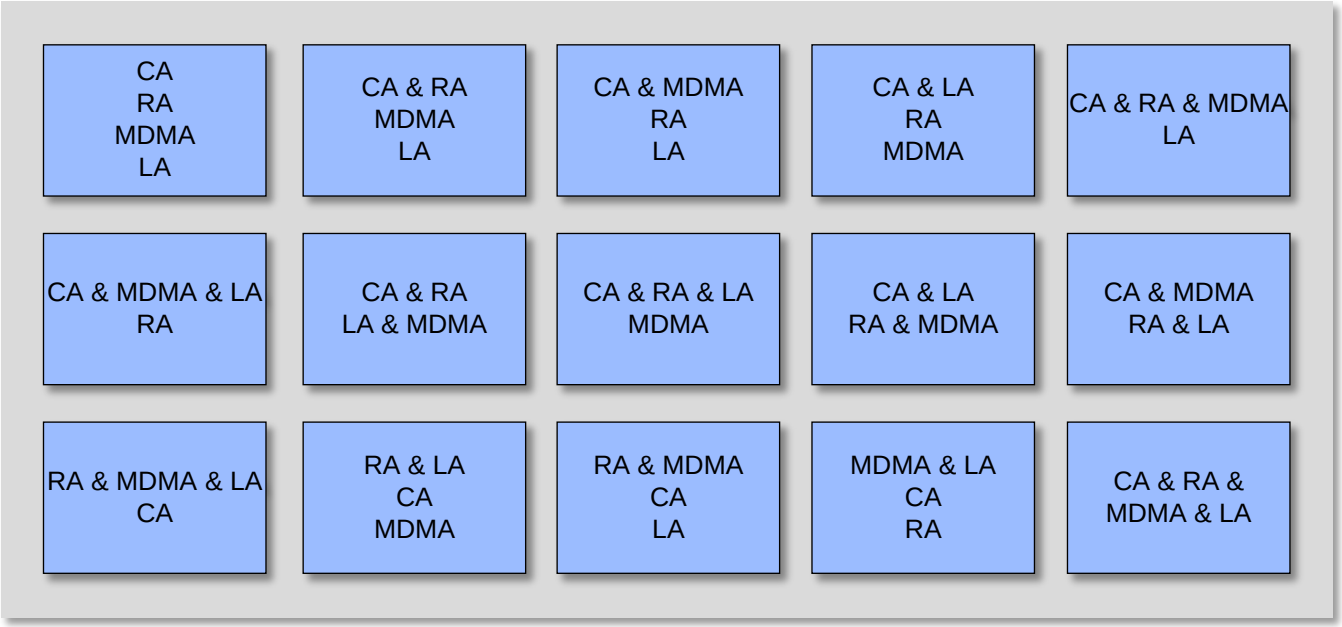
Functions of Use



Roles and responsibilities for each model are commensurate with the activities and sub functions per function that are described here

All Possible CME Organizational Models

There are 15 unique ways to design the organizational model for the CMEs. Models include different combinations of the four functions involved in certificate management



- All possible combinations of the CA, RA, LA, and MDMA were explored
- Models were evaluated based on communications security and privacy protections, as well as organizational factors to determine acceptability

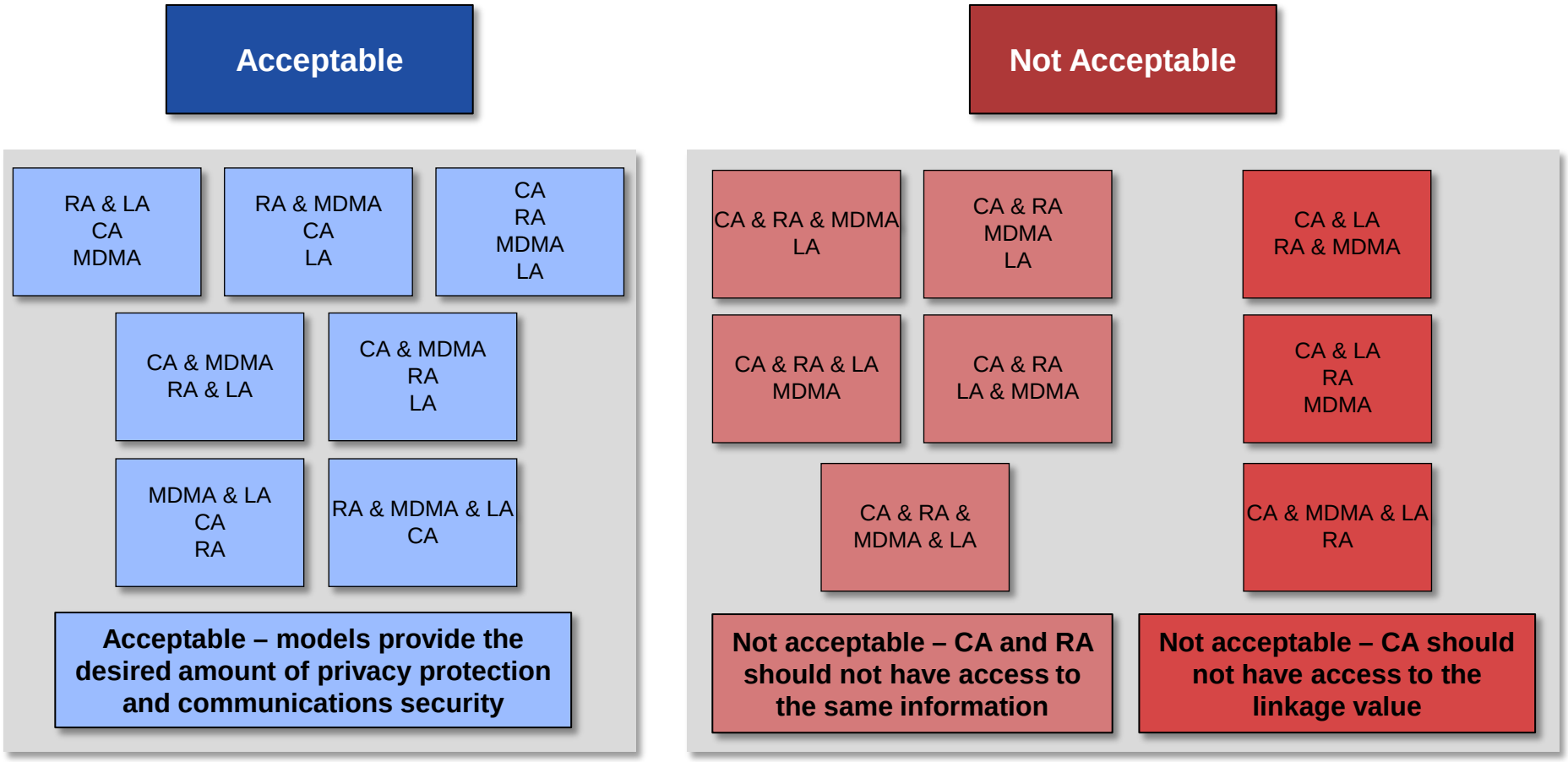
Key

- **CA**: Certificate Authority
- **RA**: Registration Authority
- **LA**: Linkage Authority
- **MDMA**: Misbehavior Detection and Management Authority

+ CA_{ACT} RA_{ACT}

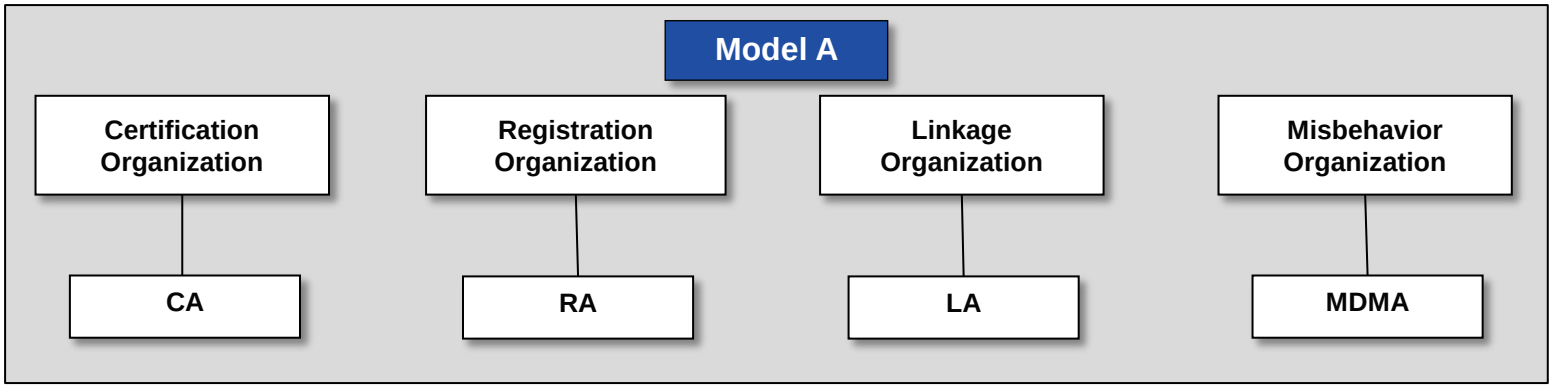
CME Organizational Model Breakdown

To ensure security and privacy within the CME, a subset of the organizational models were eliminated from the list of those considered. Seven models were deemed acceptable for consideration



Model A – Four Separate Entities

+ CA$_{ACT}$ RA$_{ACT}$



Advantages

- Provides the strongest security and privacy protection
  - Creates the greatest amount of complexity to effectively deter hackers
  - Minimizes risk of operators/overseers colluding to misuse data
  - Ensures no one entity has access to the full amount of data that would allow for security breaches

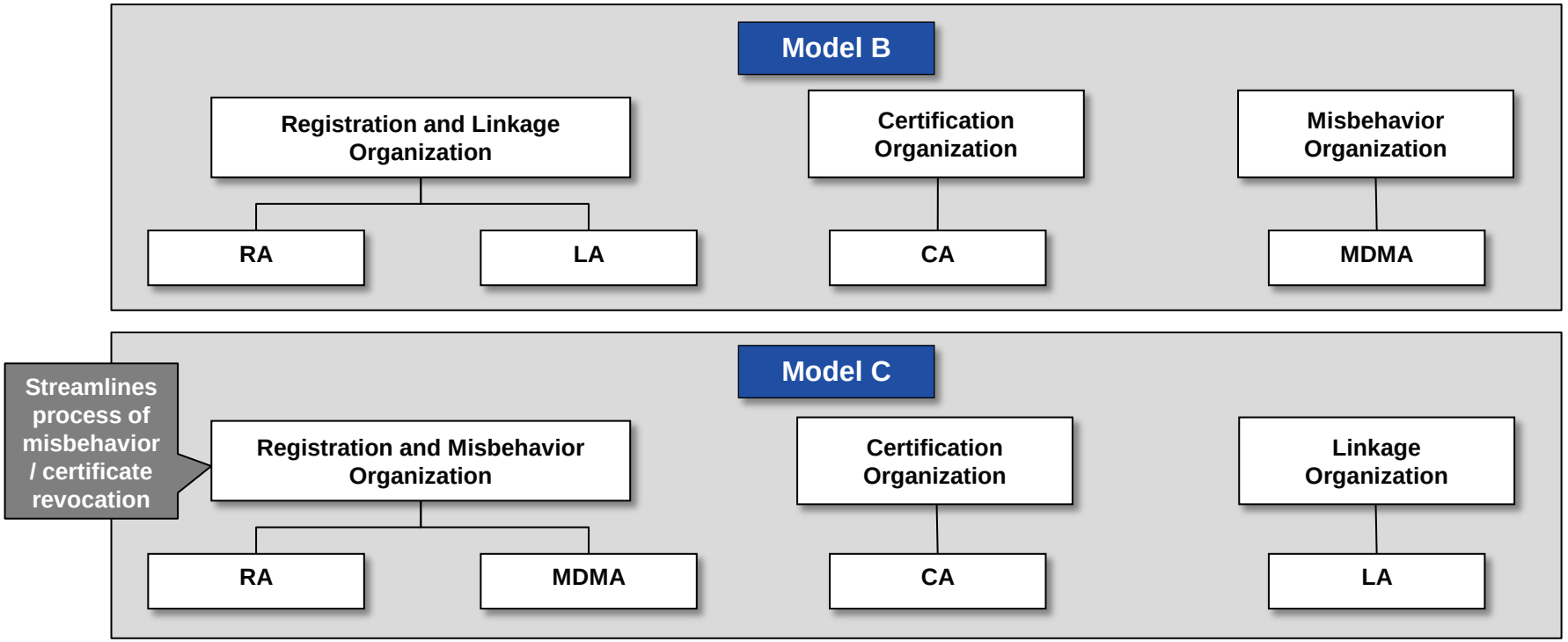
Disadvantages

- Increases costs and amount of needed resources, staff, and IT
- Requires additional level of effort to achieve inter-organization collaboration and communication
- Increases organizational and management complexity

Separating each function into a standalone organization/entity was recommended by one stakeholder group to ensure maximum privacy protection and communications security

Models B & C – Two Combined, Two Separate

+ CA_{ACT} RA_{ACT}



Advantages

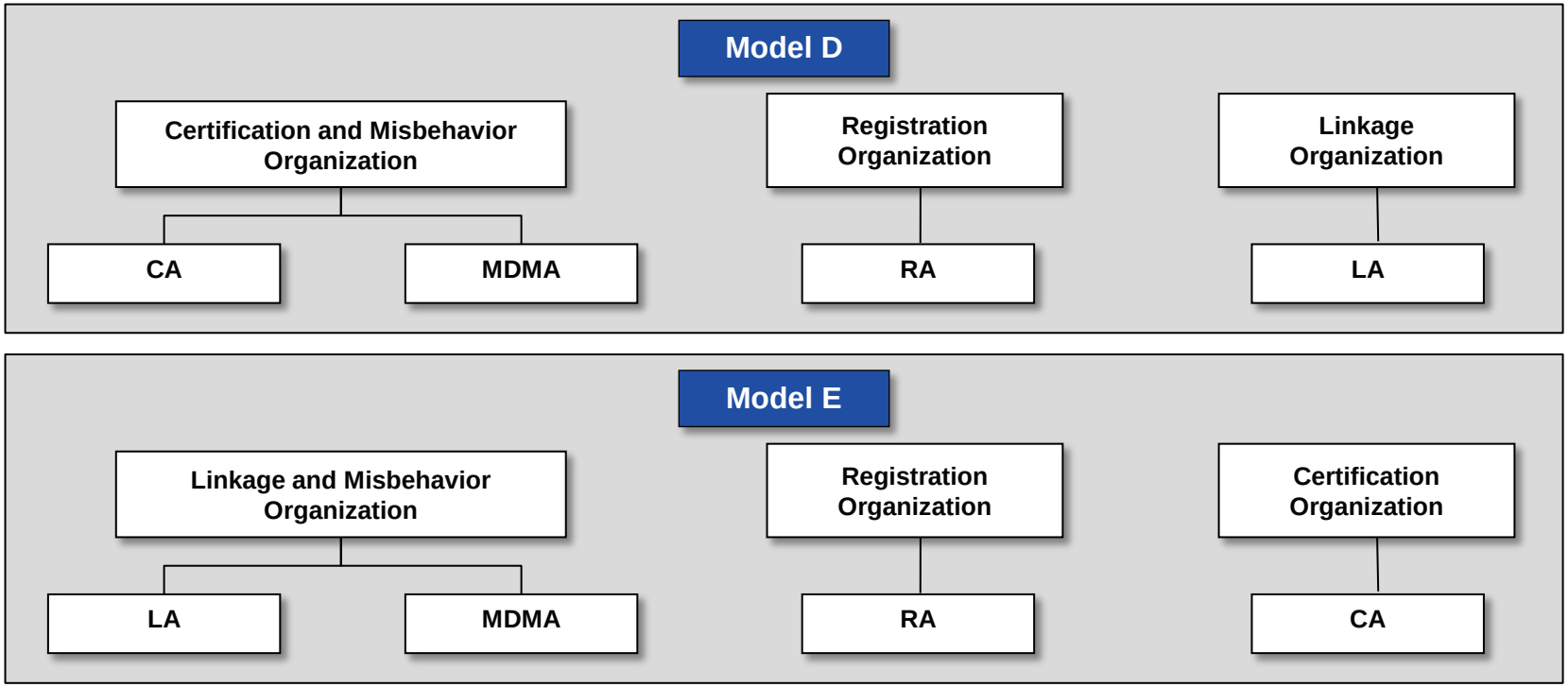
- Maintains security and privacy protection
- Decreases operational complexity
- Decreases costs and need for additional resources

Disadvantages (Relative to Option A)

- Increases vulnerability to security breaches that would cause system interruptions or denial of service. This may also allow for malicious vehicle tracking to occur due to the potential for access to additional information

Models D & E – Two Combined, Two Separate

+ CA_{ACT} RA_{ACT}



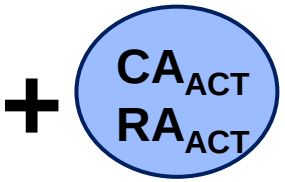
Advantages

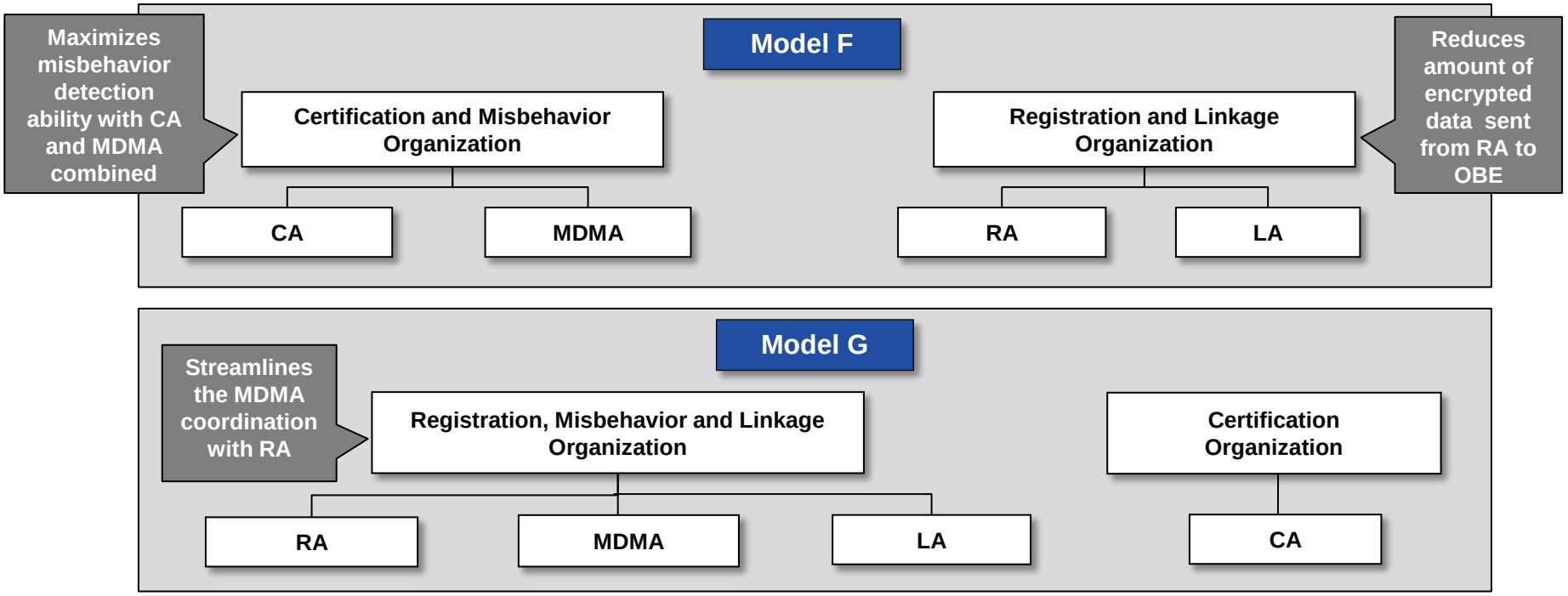
- Maintains security and privacy protection
- Decreases operational complexity
- Decreases costs and need for additional resources

Disadvantages (Relative to Option A)

- Increases vulnerability to security breaches that would cause system interruptions or denial of service. This may also allow for malicious vehicle tracking to occur due to the potential for access to additional information

Models F & G – Two Combined





Advantages

- Decreases costs and need for additional resources
- Simplifies inter-organization communications and collaboration

Disadvantages (Relative to Option A)

- Increases vulnerability to security breaches that would cause system interruptions or denial of service. This may also allow for malicious vehicle tracking to occur due to the potential for access to additional information

Comparative Research

Technical Guidelines

Highlighted technical elements within a PKI system that impact the operation of a CME

- Key elements for solid PKI governance include a Certificate Policy, Certification Practice Statement, and Cross Certification Agreements (when multiple PKIs are involved)
- Communication between entities should adhere to industry standards such as ITU-T X.509
- Privacy standards such as the Payment Card Industry Data Security Standard (PCI-DSS) can help guide development of PII policy for the unique requirements of the CME

Industry Governance

Organizations or programs spanning multiple jurisdictions that illustrate coordinated efforts and simultaneously meet the needs of multiple parties

- **E-ZPass Interagency Group** – The body coordinating toll collection across14 states in the Northeast United States
- **International Registration Plan (IRP)** – An agreement within the Trucking Industry that ensures registration fees are justly apportioned amongst states where motor carriers travel
- **National Strategy for Trusted Identities in Cyberspace** – A Federal program creating an "Identity Ecosystem" within the Internet to ensure cyber security for citizens across the US

PKI Industry Leaders

Private sector firms offering PKI expertise

- **Symantec** – A global PKI leader, owner of *VeriSign® Certificate Lifecycle Platform from Symantec*
- **Entrust** – A Federal Government partner that has worked closely to develop the Federal Bridge Certification Authority (FBCA)
- **IdenTrust** – A Federal Government partner that has supported PKI efforts at both the federal and state level, particularly within the DoD

Industry Governance

- Any of the models conceptualized here will have to be overseen and governed by an industry governance structure that will decide on standards, policies, compliance, and related guidelines
- Industry governance determines and manages issues that affect all organizations involved in certificate management. These issues include (but are not limited to):
  - Required levels of privacy protection
  - Required levels of communications security that must be implemented and maintained
  - Standards and guidelines for competition
  - Quality standards – levels of service, responsiveness to questions and complaints
  - Connection to law enforcement or other potentially related organizations
  - Research and development standards and policies

Public	Private	Hybrid
Organizations operated by and standards decided on by federal, state, and/or municipal government(s) agencies or representatives. Funded by tax dollars	Organizations operated by and standards decided upon by non-government agency or association of agencies. Funding from non-tax dollars	Public/private partnerships created in order to leverage expertise from industry leaders while addressing policy issues that accompany the development technologies, programs, systems, or standards

Examples of Industry Governance Structures

Public Governance Model

- **Federal PKI Policy Authority (FPKIPA) Steering Committee** – The agency responsible for managing the Federal Bridge Certification Authority (FBCA) and setting the Certificate Policies for the government's PKI cross certification system

Private Governance Model

- **AICPA Auditing Standards Board** – The body that issues auditing, attestation, and quality control statements, standards and guidance to CPAs for non-public company audits. AICPA ensures adherence to Security and Exchange Communications regulations (*AICPA website*)

Hybrid Model

- **Smart Grid Interoperability Panel** – A panel of stakeholders led by NIST to develop standards for the implementation of SmartGrid technology across the US during the 21st century
- **E-ZPass Interagency Group** – 24 toll agencies in 14 states manage fee collection for more than 21 million radio-frequency identification (RFID) transponders
- **ICANN Board Governance Committee** – A non-profit public benefit corporation created to keep the Internet secure, stable, and interoperable. The federal government has a say in its ability to set policies for the internet (*ICANN website*)

CME Organizational Governance

- Organizational governance refers to the set of **decisions, oversight, management, leadership, and organizational standards** that must exist in any organization to provide **authority and accountability, as well as strategic direction**
- Different governance structures have varying and significant effects on **how staff and managers behave**, how various operating **rules and guidelines** facilitate the necessary outcomes, and how **performance is evaluated**
- In addition, **compliance with standards, policies and guidelines** are all part of what an organizational governance structure is tasked with overseeing

Key Organizational Governance Questions:

- How many levels of hierarchy exist
- How different divisions and units coordinate and report outcomes
- Who holds decision-making authority for different kinds of decisions (e.g. hierarchical and functional divisions for strategic versus operational decisions)
- Who decides on standards, strategic goals, and evaluation practices
- Who has ultimate accountability for different kinds of decisions and operations

Evaluation Criteria

Evaluation criteria are based on high level organization design models and anticipated technical guidelines (as determined by current working assumptions)

Criteria	Description
Security	How well a model ensures availability, integrity and security of communications
Privacy	How well a model protects user's privacy
Cost (Reverse Scale)*	What are the relative levels of costs associated with each model
Longevity of Policy/System	How long before policy/system will need to be updated
Scalability - Technical Ease	How well a model is anticipated to scale technically
Scalability - Resource Needs (Reverse Scale)	How heavy are the resource requirements for scaling the model
Anticipated Support	Expectations of stakeholder group supporting model implementation
Technical Feasibility	Anticipated ease of technical implementation
Ability of Testing	How practical it is to test the model
Organizational Simplicity	How simple the organization is to operate
Encouragement of Participation	How well a model encourages high levels of participation (both after CRL and as opt-in)

Based on Design Requirements (see Appendix)

** Evaluation of implementation options, such as integrating certain functions into existing organizations (e.g. vehicle registration) will impact cost estimates during the second phase of this project*

Summary

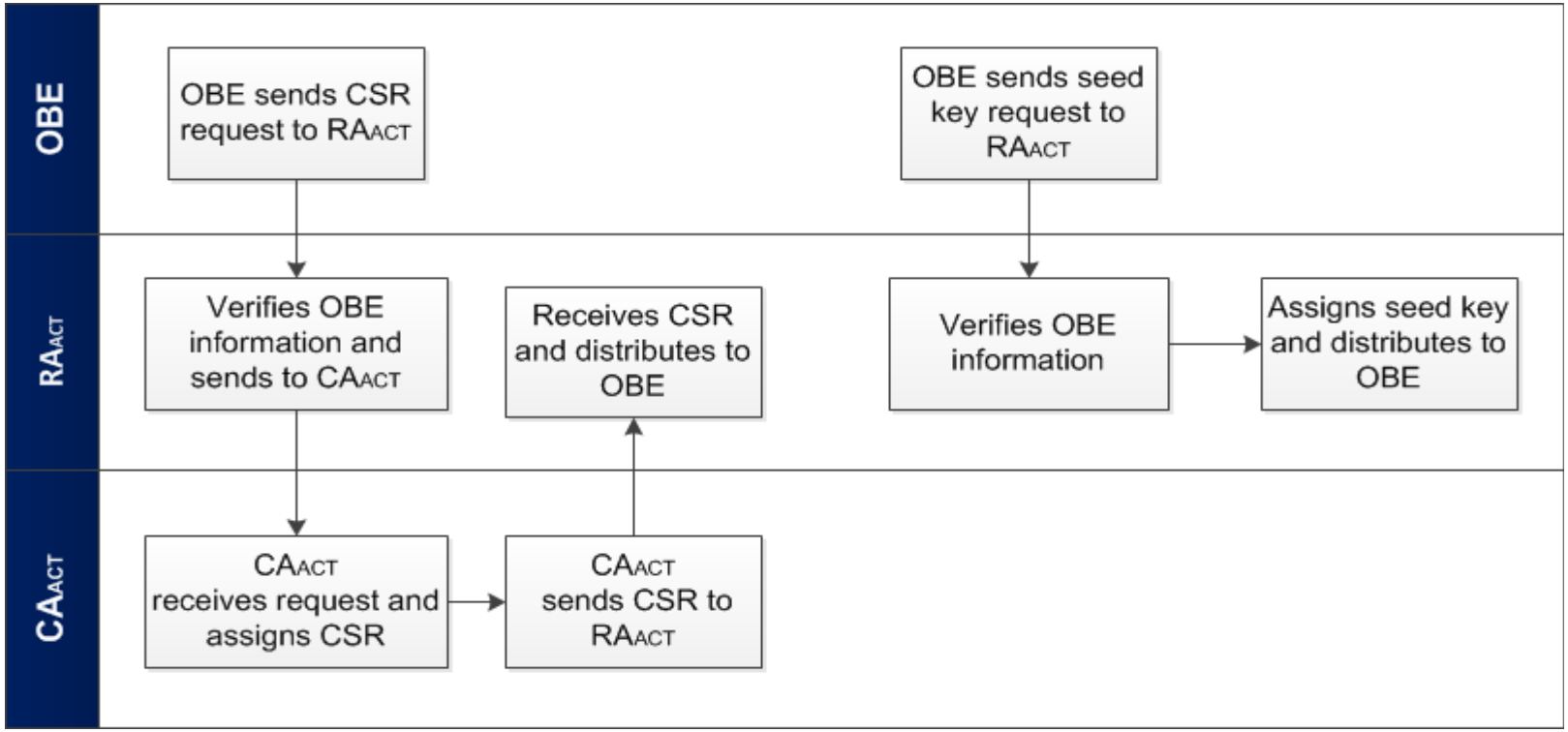
A review of the model options reveals the following initial findings:

- **Model A**, with four separate entities representing each of the four functions, is unique because of its high and low ratings
  - It ensures privacy and security to the fullest, but is also estimated to be the most costly and difficult to implement and scale
  - There is no technical reason to believe that MDMA should ever be separate as it does not hold or use any information that can be used for tracking devices or violating privacy
- **Models B, C, D, and E**, with two functions combined into one entity and with two separate entities for the other two functions, are comparable in their ratings
  - While the different combinations of functions can potentially save costs, some are more effective than others due to the similarity of the activities performed by the functions
  - Model C, with RA and MDMA together, provides a streamlined functionality for misbehavior detection and certificate revocation
- **Models F and G**, with two separate entities made up of different combinations of the functions, are comparable in their ratings
  - These model options offer other possibilities for cost savings and coordination of functional activities, but may pose challenges to execution
  - Model F maximizes misbehavior detection because of the CA and MDMA combination, and also reduces the amount of encrypted data going from RA to OBE
  - Model G streamlines the MDMA and RA coordination (as in C above) but with additional organizational efficiencies due to the placement of LA within the same entity

Appendix

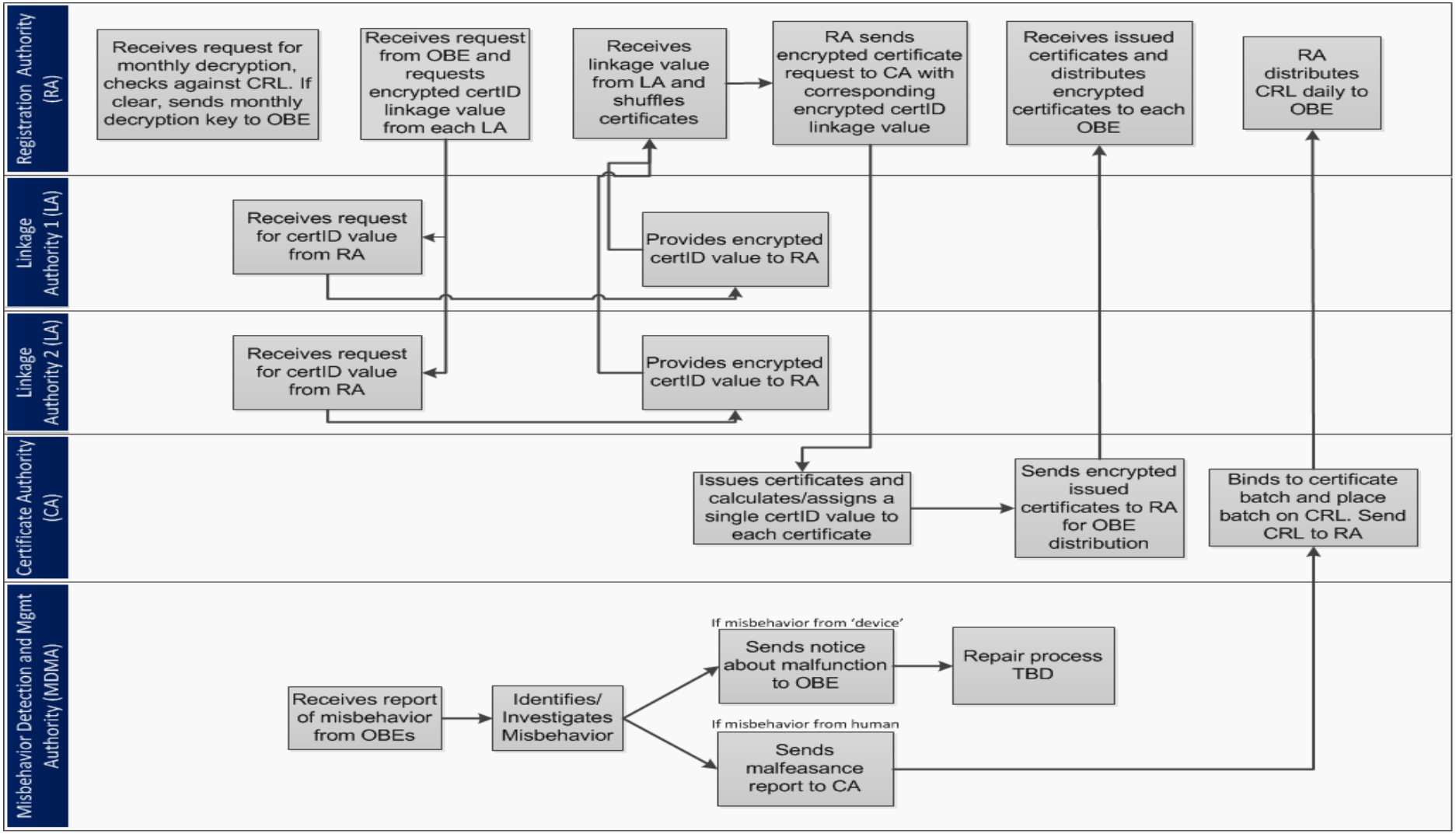
Activation Phase: Certificate Signing Request and Seed Key Sub-Functions

CA_{ACT} and RA_{ACT} are functions related to the request and assigning of Certificate Signing Request certificates and Seed Keys which activate the OBE



There will be a Certificate Revocation List (CRL) produced for CSR certificates. The dissemination of the CRL and the CSR connection to the pseudo system MDMA will be developed as the technical architecture and policy decisions evolve

Use Phase – Basic Functions



Design Requirements for the CME Options

Design Requirements	Source of Requirement
All data exchanges and communications between devices must be encrypted, secure and reliable	▸ All technical architecture docs ▸ Inherent need of a large, high volume, public communications system
Governance of the CMEs must be reliable and trustworthy	▸ Best practices for sustainable organizations
Privacy of individuals in the system must be protected appropriately	▸ Fair Information Practices Principles ▸ Stakeholder Input
Funding of the CMEs should not be burdensome to any one group	▸ Resource constrained environment and estimates of future funding constraints ▸ Stakeholder Input
The system should be easy to use for individuals	▸ Commonly accepted usability requirements

These design requirements provide the foundation for how the organizational and operational options will be configured to address the needs of various stakeholder groups and technical requirements. This will also be used as the basis for evaluating the different models